What are the PCI Rules for storing credit card data?

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

Introduction

More than often when software developers design platforms for digital payments, they are unaware of why and how the applications are used for handling card holder data (CHD). On the other hand, most merchants are not aware of whether these applications store CHD. This results in unencrypted data storage and exposure to various cyber threats. While some Merchants may have to store sensitive cardholder data for payment processing, transaction history, or recurring billing, it is important that the developer is aware of such requirements and accordingly designs applications with the necessary security measures for safe handling such sensitive data. Addressing these issues the PCI Council along with the support of major card brands developed the Payment Card Industry Data Security Standard (PCI-DSS).

The Standard which is a widely accepted set of requirements ensures optimum security of sensitive cardholder data and protection against evolving cyber threats. PCI-DSS requirements apply to all entities that store, process, or transmit cardholder data. The requirements outlined clearly state that cardholder data can only be stored for a "legitimate legal, regulatory, or business reason." So for those businesses that have a legitimate reason to store data must understand the PCI requirements and know what measures they must take to protect that data. Elaborating the PCI requirements in detail our article explains the PCI Rules that vendors and merchants must follow for storing sensitive credit card data. So, let us first take a closer look at the PCI Guidelines for Data Retention.

PCI Guidelines for Data Retention

Merchants must avoid storing cardholder data unless they have a legitimate legal, regulatory, or business reason to do so. That said, the data classified as the Cardholder Data (CHD) which includes the 16-digit primary account number (PAN), cardholder name, service code, and expiration date are the kind of data that can probably be stored. However, it is important to note that the Sensitive Authentication Data (SAD) cannot be stored after authorization of a transaction, even after encryption. Data that is classified SAD include the full magnetic stripe data found on the back of the card, data on the EMV chip, the CVV, PIN, and PIN block. SAD data are extremely valuable and should be protected at all costs for it is a valuable tool for attackers to use the card-present and card-not-present environment.

So, to ensure maximum protection of sensitive data, Merchants should develop a data retention and storage policy that strictly limits storage and retention time based on the business, legal, and/or regulatory requirement. Further, Merchants must also implement necessary PCI DSS requirements and ensure general protection of the cardholder data environment.

	Data elements	Storage Permitted	Protection Required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	Yes
	Service Code	Yes	Yes
	Expiration Date	Yes	Yes
Sensitive Authentication Data	Full Magnetic Strip Data	No	N/A
	CAV2/CVC2/CVV2/CID	No	N/A
	PIN/PINBlock	No	N/A

Source - ***PCI SSC***

What does PCI say about Data Storage?

The PCI DSS outlines in its Requirement 3, guidelines to protect stored cardholder data. Requirement 3 applies only if the Merchant stores the cardholder data. Merchants who do not store cardholder data have stronger protection against the threat as they eliminate the primary target for hackers. While merchants who have a legitimate business reason to store Cardholder Data, need to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. For getting a better perspective and understanding of PCI DSS Require 3, let us take a closer look at the PCI rules for the storage of data.

PCI Rule for Storage of cardholder data

Focusing on the PCI Requirement 3, it provides guidelines for protecting stored Cardholder Data. Requirement 3 constitutes multiple sub-requirements that the Merchants are required to understand and follow. It is important that Merchants who own the responsibility of securing Cardholder Data must understand the requirements outlined and know the differences between Account Data, Cardholder Data, and Sensitive Authentication Data. While the Account Data constitutes all the data that is there on a credit card, the Cardholder Data (CHD) includes the 16-digit PAN, expiration date, and cardholder name, and the Sensitive Account Data (SAD) includes sensitive track data the magnetic stripe, CVV, PIN, and PIN Block. SAD data is very sensitive data that cannot be stored after authorization. If at all, SAD storage is allowed only for issuers for the purpose of testing and error correction. Storage of cardholder data should be limited to what is necessary and only to meet legal, regulatory, or business needs. Given below are PCI Rules outlined with a detailed explanation of the requirement and what is expected of the merchants to ensure the protection of stored cardholder data.

PCI Rules	Explanation
PCI Rule 3.1- Keep Cardholder Data Storage to Minimum	PCI-DSS requirement 3.1 clearly states that the Cardholder Data should be limited to what is necessary for legal, regulatory, or business needs. The requirement also states that entities must develop data retention policies, secure deletion policies, and every quarter identify and remove any Cardholder Data that exceeds the retention period. A data discovery tool may be used for identifying such data. Entities must define measures to delete the data securely when no longer needed.
PCI Rule 3.2- Do Not Store Sensitive Authentication Data After Authorization	PCI-DSS requirement 3.2 states that Sensitive Authentication Data (SAD) cannot be stored after authorization, even if it is encrypted. The data must be immediately deleted and ensured it is unrecoverable after the authorization process. SAD includes the full track data, CVV, and PIN data that are extremely valuable to attackers. Unauthorized access to such sensitive data can lead to fraudulent transactions over both card-present and card-not-present transactions. Only payment card issuers or entities that have a legitimate business need related to the issuing services can store the data.
PCI Rule 3.3- **Mask Primary Account Number (PAN) When Displayed**	PCI DSS requirement 3.3 states that the PAN number must be masked when displayed. PNA number is the 16 digit number displayed at the front of the card. The requirement clearly states that not more than the first six and last four digits number must be displayed. Only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. The entity must establish a policy and procedure that ensures the masked display of PAN.
PCI Rule 3.4 Make PAN Unreadable Wherever Stored	PCI DSS requirement 3.4 states that the PAN Data that is stored for an unavoidable reason must be rendered unreadable wherever it is stored. The PCI-DSS explicitly elaborates some of the acceptable methods for rendering the PAN data unreadable. This includes Hashing, Truncation, or Encryption methods. While the hashed index method simply involves displaying only the index data that point to records in the database where the sensitive data resides, truncation involves removing a data segment by simply displaying only the last four digits. Index token on the other hand is an encryption algorithm that combines sensitive plain text data with a random key or pad to render the data unreadable. Strong cryptography is another method that involves using mathematical formulas to render plain text data unreadable. PAN data rendered unreadable makes it extremely difficult and time-consuming to decrypt the data and difficult for attackers to hack.

PCI Rule 3.5 Protect Keys Used To Store Cardholder Data	PCI DSS requirement 3.5 states the use of cryptography and requires entities to take measures to protect encryption keys from disclosure and misuse. Data that are encrypted can be decrypted if the attacker gains access to encryption keys. For these reasons, the encryption keys must be developed strong and stored separately in the least possible location and form with limited access granted to individuals. While securing the encryption key entities must consider both external threats and the internal threats from employees. Further, entities are expected to document a description of the cryptographic architecture including details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date, description of the key usage for each key, and an inventory of any HSMs and other SCDs used for key management.
PCI Rule 3.6 Document and Implement all Key Management Processes and Procedures for Encryption Keys Used to Encrypt Cardholder Data	PCI DSS requirement 3.6 states that the entities must build key management programs and document every aspect of key management including the process, procedures, and implementation of encryption keys used for encrypting cardholder data. This includes the secure generation, distribution, and storage of cryptographic keys and policies that require key changes at the end of the crypto period or if the integrity of the key is compromised or weakened due to various reasons. Establishing a good Key Management Process is essential be it manual or automated as part of the encryption product based on industry standards to ensure all key elements stated in requirement 3.6 are addressed.
PCI Rule 3.7 Security Policies and Operational Procedures are Documented and Communicated to all the Affected Parties	PCI DSS requirement 3.7 states that the entities must have in place policies and procedures that are not just documented but also communicated to individuals involved in the protection of Cardholder Data (CHD) and also ensure that they are enforced and duly followed. The policies and procedures should just be documented for the sake of the audit. Entities must ensure that these policies and procedures are well understood by the employees and made aware of their responsibility towards the protection of CHD.

It is important to note that these above listings are the direct controls for stored card data. However, there are a few other controls such as network controls, hardening requirements of the assets, and even what can be seen in requirement 10 of PCI DSS that mandates the logging and reporting required for all access to card data.

Conclusion

Merchants and Payment Application Developers must both be aware of the requirements and understand how and why the digital payment solutions handle cardholder data (CHD). They must also establish strong security measures to protect stored cardholder data as per the PCI-DSS compliance requirements. Further, to fulfill the Require 3 of **PCI DSS Compliance** we strongly recommend Merchants reduce their PCI scope by streamlining the card data flow, storing only data that is necessary, and implementing network segmentation to reduce the risk exposure from the rest of the network¬.

Orginally published on:- Financederivative

Written By:- VISTA Infosec

Do write to us your feedback, comments and queries or, if you have any requirements: info@vistainfosec.com

You can reach us on:

USA	INDIA	SINGAPORE	UK
+1-415-513 5261	+91 73045 57744	+65-3129-0397	+442081333131